

**PENGURUSAN RANGKAIAN:  
ANALISIS TAHAP KESIHATAN RANGKAIAN KOMPUTER UUM  
BERASASKAN ANALISIS PAKET**

**Projek ini dikemukakan kepada Sekolah Siswazah  
sebagai sebahagian keperluan penganugerahan  
Ijazah Sarjana Sains (Teknologi Maklumat)  
Universiti Utara Malaysia**

**Oleh  
Rosmadi Bin Bakar**

**©Rosmadi bin Bakar, 2001. Hak Cipta Terpelihara**



**Sekolah Siswazah  
(Graduate School)  
Universiti Utara Malaysia**

**PERAKUAN KERJA KERTAS PROJEK  
(Certification of Project Paper)**

Saya, yang bertandatangan, memperakukan bahawa  
(I, the undersigned, certify that)

**ROSMADI BIN BAKAR**

calon untuk Ijazah

(candidate for the degree of) Sarjana Sains (Teknologi Maklumat)

telah mengemukakan kertas projek yang bertajuk  
(has presented his/her project paper of the following title)

**PENGURUSAN RANGKAIAN: ANALISIS TAHAP KESIHATAN RANGKAIAN**

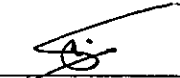
**KOMPUTER UUM BERASASKAN ANALISIS PAKET**

seperti yang tercatat di muka surat tajuk dan kulit kertas projek  
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan,  
dan meliputi bidang ilmu dengan memuaskan.

(that the project paper acceptable in form and content, and that a satisfactory  
knowledge of the field is covered by the project paper).

Nama Penyelia : En. Ahmad Suki bin Che Mohamed Arif  
(Name of Supervisor)

Tandatangan :   
(Signature)

Tarikh : 25/11/2001  
(Date)

## **KEBENARAN MENGGUNAKAN TESIS**

Laporan ini merupakan sebahagian daripada syarat pengijazahan program pasca Sarjana Sains (Teknologi Maklumat), Universiti Utara Malaysia. Dengan ini saya bersetuju membenarkan pihak perpustakaan mempamerkan laporan ini sebagai bahan rujukan umum. Saya juga bersetuju membenarkan mana-mana pihak membuat salinan samada sebahagian atau keseluruhan projek ini bagi tujuan akademik dengan syarat mendapat kebenaran terlebih dahulu daripada penyelia projek ataupun melalui Dekan Sekolah Siswazah, Universiti Utara Malaysia. Sebarang bentuk cetakan atau salinan bagi tujuan komersil adalah dilarang tanpa merujuk kepada penyelidik.

Kebenaran perlu diperolehi terlebih dahulu untuk menyalin atau menggunakan samada sebahagian atau keseluruhan isi kandungan projek ini. Rujukan kepada penulis dan Universiti Utara Malaysia perlu dinyatakan dalam sebarang laporan bagi tujuan rujukan sebagai ulasan karya.

Dekan Sekolah Siswazah  
Universiti Utara Malaysia  
06010 Sintok, Kedah.

## Abstrak

Rangkaian telah wujud lama sebelum komputer menjadi kenyataan. Pada tahun 1846 Samuel F. B. Morse telahpun mencipta kod digital. Dalam tahun 1876 Alexander Graham Bell pula telah mendaftar paten bagi telefon. Manakala tahun 1878 rangkaian suara pertama telah dibina. Pada tahun 1970an IBM telah memperkenalkan rangkaian komputer berpusatkan host kerangka utama yang dikenali sebagai SNA dan Xerox memperkenalkan konsep ethernet. Penggunaan rangkaian komputer semakin menjadi keperluan seiring dengan perkembangan teknologi internet. Pada hari ini setiap komputer perlu dirangkaian dalam sistem rangkaian komputer. Dengan sistem rangkaian ini berbagai maklumat dan sumber boleh dikongsi bersama. Bagi sesetengah sektor seperti sektor perindustrian, perbankan, perniagaan, telekomunikasi dan keselamatan, rangkaian komputer menjadi nadi kepada aktiviti mereka. Kegagalan sistem rangkaian berfungsi beerti lumpuh perjalanan dan operasi mereka. Oleh itu pengurusan rangkaian yang cekap perlu diperkenalkan agar konfigurasi rangkaian dapat dilaksanakan dengan tepat dan pengurusan kerosakan dapat dilakukan dengan baik agar prestasi rangkaian dapat mencapai tahap yang memuaskan. Satu daripada kaedah bagi pengurusan rangkaian ialah dengan menganalisis sistem rangkaian berasaskan analisis paket. Dengan menganalisis paket atau protokol ini beberapa fenomena dapat dikenalpasti. Kajian ini ialah bertujuan menganalisis sistem rangkaian komputer Universiti Utara Malaysia Sintok (ISLAN). Ojektif kajian ini ialah membuat capture paket yang melalui rangkaian komputer ISLAN bagi mengenalpasti jenis-jenis paket berasaskan protokol penghantaran, bentuk-bentuk paket seperti saiz dan formatnya, paket-paket yang menyebabkan kesesakan kepada rangkaian, cara penghantaran paket, paket-paket yang dijanakan dan melalui rangkaian pada waktu-waktu tertentu seperti waktu penggunaan rendah, sederhana dan puncak, selain itu ialah untuk mengenalpasti paket-paket yang dijanakan oleh sistem rangkaian sendiri untuk tujuan pengaktifan rangkaian oleh sesuatu protokol, meninjau laluan paket, dan menyukat penggunaan *bandwidth*. Penganalisan ini menggunakan perisian Sniffer Pro bagi tujuan *capture* dan analisis. Dapatan kajian mendapati terdapat perbezaan jumlah paket diantara waktu-waktu penggunaan tertentu, hari bekerja dan hari cuti, segmen kakitangan dan pelajar. Bagaimanapun didapati tiada perbezaan yang ketara berbanding pelbagai lokasi. Didapati sangat banyak paket yang dihantar secara *broadcast* dari segemen lain dan tersebar keseluruh rangkaian yang membabitkan *bandwidth* rangkaian. Walaubagaimanapun, didapati *bandwidth* yang digunakan oleh sistem rangkaian sangat rendah. Daripada menganalisis paket tersebut tahap kesihatan rangkaian dapat diuraikan dan maklumat yang diperolehi akan memungkinkan untuk mendapatkan kaedah bagi penyelesaian kepada masalah-masalah berkaitan.

## **Abstract**

Network existed long before computers became a reality. In 1846 Samuel F.B.Morse invented the digital code, in 1876 Alexander Graham Bell registered the telephone patent and in 1878 the first voice network was established. In the nineteen seventies IBM introduced the computer network which was based on the mainframe host known as SNA while Zerox introduced the concept of Ethernet. The utilization of computer network has increasingly become a necessity in line with the development of internet technology. Today every computer needs to be connected to the computer network system . With this network, varieties of information and sources can be shared. For certain sectors such as industrial, banking, business, telecommunication and security, computer network is the catalyst to their activities. If the network system fails to function, their operations will be crippled. Thus, efficient network management needs to be introduced so that network configuration can be executed accurately and management of defects can be carried out effectively in order that the network performance can be maintained at a satisfactory level. One of the methods to manage the network is to analyze the network system based on the packet analysis or protocol analysis. Through this method or protocol, several phenomena can be identified. This study aims to analyze the Northern University of Malaysia Computer Network System(ISLAN). The objective of the study is to provide packet capture through ISLAN computer network in order to identify packet types based on delivery protocol, types of packet such as size and format, packet which cause congestion in the network, methods of packet delivery, packet which are generated and passed through the network at certain times such as low, moderate and peak utilization periods. It also aims to identify the packet generated by the system itself for the purpose of activating the system by certain protocol, surveying the packet route and measuring the utilization of the bandwidth. The analysis uses Sniffer Pro software for capture analysis. The study reveals that there are differences in the number of packet among certain utilization periods, work days and holidays, student and staff VLAN segments. Nevertheless there are no obvious differences among the various locations. A large number of packet are sent through broadcast from other segments and distributed to the whole network which involved network bandwidth. However, the bandwidth used by the system is very low. Based on the packet analysis, description of the network fitness level is done and the information obtained will help identify ways to solve the related problems.

## **PENGHARGAAN**

Alhamdulillah syukur ke hadrat Allah S.W.T yang sentiasa memberi taufik dan hidayahNya serta ketabahan kepada penulis sehingga selesai menyiapkan projek ini.

Pada kesempatan ini, penyelidik merakamkan penghargaan istimewa buat Encik Ahmad Suki bin Che Mohamed Arif selaku penyelia yang amat komited, sentiasa bersedia dan bersemangat dalam memberi tunjuk ajar, bimbingan dan saranan yang membina dan amat bernilai dari awal kajian hinggalah terhasilnya projek ini. Terima kasih juga kepada rakan sepengajian Encik Azman bin Aziz yang banyak membantu.

Ucapan terima kasih juga kepada Universiti Utara Malaysia yang telah menaja pengajian dan memberi cuti belajar kepada penyelidik. Terima kasih juga buat para pensyarah yang telah memberi tunjuk ajar sepanjang pengajian, rakan-rakan seperjuangan yang sentiasa membantu serta kenalan-kenalan di Universiti Utara Malaysia yang memberi sokongan dan dorongan untuk meneruskan dan menamatkan pengajian ini.

Akhir sekali, penghargaan dan rasa kasih sayang paling istimewa buat isteri, Nafisah Mahmud dan anak-anak Awanis, Amalia, Atirah, Azim dan Adibah. Juga kepada umi dan baba, emak dan ayah, serta adik beradik dan ipar duai yang sentiasa menyenangkan penyelidik.

Hanya Allah yang dapat membalas segala budi dan jasa yang diberi. InsyaAllah, semoga Allah memberkati segala usaha kita.

## **DAFTAR KANDUNGAN**

## **HALAMAN**

Kebenaran menggunakan Tesis	i
Abstrak	ii
Abstract	iii
Penghargaan	iv
Daftar Kandungan	v
Senarai Jadual	viii
Senarai Rajah	ix
Senarai Lampiran	x
Senarai Singkatan	xi

## **BAB 1      PENDAHULUAN**

Pengenalan	1
Rangkaian Komputer UUM	5
• Rekabentuk Rangkaian Uum	5
• Teknologi Transmisi	7
• Perkakasan Rangkaian	8
• Aplikasi Yang Digunakan	10
Pernyataan Masalah	12
Objektif Kajian	14
Persoalan Kajian	15
Kepentingan Kajian	16
Batasan Kajian	18
Defini Operasional	19

## **BAB 2      SOROTAN PENULISAN BERKAITAN**

Pengenalan	21
Rangkaian Komputer	21
• Jenis-Jenis Rangkaian	24
• Piawaian Dan Protokol	26
• Model Rujukan Osi	28
Penganalisis Protokol ( <i>Protocol Analyzer</i> )	37
• Komponen ' <i>Paket Sniffer</i> '	39
• Asas Operasi Penganalisis Protokol	40
• Perbezaan Antara Penganalisis Protokol	44
Kaedah <i>Browsing</i> Trafik Internet	46
Protokol Rangkaian Microsoft	47
Kesimpulan	49

## **BAB 3      METODOLOGI KAJIAN**

Pengenalan	50
Rekabentuk Kajian	50
Pembolehubah Kajian	51
Populasi dan Sampel	51
Instrumen Kajian	52
Pengumpulan Data	54
Analisis Data	55
Kesimpulan	56



## **BAB 4        DAPATAN KAJIAN**

Pengenalan	57
Profil Paket (Tanpa Menggunakan Aplikasi)	58
Capture Paket Pada Hari Bekerja	61
Capture Paket Pada Hari Cuti	64
Capture Paket Pada Pelbagai Lokasi Sekolah	67
Capture Paket Bagi VLAN Pelajar	70
Profil Paket (Menggunakan Aplikasi Tertentu)	76
Capture Paket Capaian Network Neighbourhood	76
Capture Paket Capaian Laman Web	87
Capture Paket Broadcast Segmen Lain	97
Kesimpulan	103

## **BAB 5        PERBINCANGAN, KESIMPULAN DAN CADANGAN**

Pengenalan	104
Profil Paket	105
Analisis Paket Waktu Hari Bekerja	106
Analisis Paket Waktu Hari Cuti	114
Analisis Paket Bagi Pelbagai Lokasi	117
Analisis Paket Bagi Vlan Pelajar	118
Analisis Paket Broadcast Segmen Lain	119
Analisis Paket <i>Broadcast</i> Dalam Segmen	120
Analisis Paket Capaian Pelayan Internet	121
Isu Keselamatan Melalui Analisis Paket	122
Kesimpulan	123
Cadangan	125
Cadangan Kajian Lanjutan	126

## **BIBLIOGRAFI**

## SENARAI JADUAL

JADUAL		HALAMAN
1.1	Senarai Pelayan	12
3.1	Kedudukan Lokasi Kajian	54
4.1	Paket di capture pada hari kerja	61
4.2	Paket di capture pada hari cuti	64
4.3	Paket di capture pada pelbagai lokasi	67
4.4	Paket di capture bagi VLAN pelajar	70
5.1	Rumusan kedudukan paket hari kerja	107
5.2	Rumusan kedudukan paket hari cuti	114
5.3	Perbandingan paket hari kerja dan hari cuti	115

## SENARAI RAJAH

RAJAH	HALAMAN
1.1	Rekabentuk Rangkaian UUM 6
1.2	Rekabentuk Rangkaian Satelit UUM 7
2.1-a	Topologi Bas 25
2.1-b	Topologi Gelang 25
2.1-c	Topologi Bintang 25
2.2	Model Rujukan OSI 28
2.3	Model Rujukan OSI (Fungsi Lapisan-Lapisan) 30
2.4	Penambahan <i>Header</i> Pada Data 32
2.5	Perbandingan Model OSI 34
2.6	Asas Penganalisis protokol 43
2.7	Paket Logon NT 44
4.1	Konfigurasi IP Pada Komputer 59
4.2	Konfigurasi Dengan <i>Default Setting</i> 60
4.3	Statistik paket 72
4.4	Protokol Pada Paket 73
4.5	Protokol Pada Paket Untuk IP 74
4.6	Protokol Pada Paket Untuk IPX 75
4.7-a	Paparan <i>Network Neighbourhood –Workgroup</i> SSKP 77
4.7-a	Paparan <i>Network Neighbourhood- Entire Network</i> 78
4.7-a	Paparan <i>Network Neighbourhood- Workgroup</i> PK 78
4.8	Konfigurasi <i>Define Filter</i> 80
4.9	Statistik Paket Capaian <i>Network Neighbourhood</i> 80
4.10-a-h	Decode Paket Capaian <i>Network Neighbourhood</i> 81-86
4.11-a	Laman web eweb 87
4.11-a	Laman web uum 87
4.11-a	Laman web google 88
4.12	<i>Setting define filter</i> 88
4.13	Statistik Paket Dan Protokol 89
4.14	Protokol IP 89
4.15	Protokol IPX 90
4.16a-i	Decode Paket Capaian Laman Web 90-96
4.17a-h	Decode Paket Broadcast Dari Segmen-Segmen Lain 97-102
5.1	Paket <i>announce host</i> 110
5.2	Paket <i>election browser</i> 111
5.3	Paket <i>announce browser</i> 113
5.4	Paket <i>announce host</i> 113
5.5	Paket Broadcast Dalam Segmen 120
5.6	Paket Capaian Laman Web 121
5.7	Decode Paket Data <i>Password</i> 122

## **SENARAI LAMPIRAN**

<b>LAMPIRAN</b>	<b>PERKARA</b>
<b>A</b>	Paket capture pada 210901-0355am
<b>A1</b>	Perincian Paket capture pada 210901-0355am
<b>B</b>	Paket capture pada 110901-0209am
<b>C</b>	Paket capture pada 221001-0807am
<b>D</b>	Paket capture pada 250901-0852am (Capaian ke Pelayan Internet)
<b>E</b>	Paket capture pada 240901-10:30am (Lokasi Pusat komputer)
<b>F</b>	Paket capture pada 240901-0114 tengah hari (Lokasi Makmal Komputer- SE2)

## SENARAI SINGKATAN

ARP	Address Resolution Protocol
DHCP	Dynamic Host Protocol
DNS	Domain Name System
GAN	Global Area Network
HTML	HYPER Text Markup Language
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers USA
IP	Internet Protocol
IPX	Internetwork Packet eXchange
ISO	International Standard Organization
LAN	Rangkaian Setempat (Local Area Network)
MAC	Media Access Control
MAN	Metropolitan Area Network
NIC	Kad Antaramuka Rangkaian (Network Interfaces Card)
OSI	Open System Interconnect
RFC	Request For Comment
RMON	Remote Monitoring
SMB	Server Message Block
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SPX	Sequenced Packed eXchanged
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
UUM	Universiti Utara Malaysia
VLAN	Virtual LAN
WAN	Wide Area Network

# **BAB 1**

## **PENDAHULUAN**

### **PENGENALAN**

Menurut Black (1993), Rangkaian komputer ialah sejumlah komputer ataupun terminal yang bersambungan melalui satu atau lebih laluan penghantaran (*transmission path*). Menurut Tanenbaum (1996), sesuatu sistem yang dipanggil rangkaian komputer ialah terdiri daripada sejumlah komputer yang ditempatkan pada pelbagai lokasi secara berasingan tetapi disambungkan antara satu sama lain. Sesuatu komputer itu dikatakan bersambungan jika ia dapat membuat pertukaran maklumat. Penyambungan itu boleh dibuat melalui kabel tembaga, fiber optik, gelombang mikro atau pun perhubungan satelit.

Pengurusan rangkaian membawa pelbagai maksud yang berbeza bagi orang yang berbeza. Dalam sesetengah kes, ia melibatkan perunding rangkaian komputer yang memantau aktiviti rangkaian komputer dengan pelbagai penganalisis protokol (*protocol analyzer*). Dalam kes yang lain pula, pengurusan rangkaian melibatkan *auto-polling* bagi peranti rangkaian dan komputer yang menjana paparan bergrafik dengan masa nyata (*real time*) bagi topologi rangkaian tentang perubahan yang berlaku dan keadaan trafik semasa. Secara umumnya, pengurusan rangkaian adalah perkhidmatan yang merangkumi pelbagai alatan (*tools*), aplikasi dan

The contents of  
the thesis is for  
internal user  
only

## BIBLIOGRAFI

Ahmad Mahdzan Ayob (1992). Kaedah Penyelidikan Sosioekonomi (Edisi Kedua). Kuala Lumpur. Dewan Bahasa dan Pustaka.

Briscoe, N. (Sept, 2000). Troubleshooting A Switch Network..  
<http://www.itp-journals.com> .( Mac 2001).

Chappell, L. (2000). Onsite Network Analysis. Protocol Analysis Institute.  
[http://192.41.62.222/brainshare/showdaily/sun\\_feature2.html](http://192.41.62.222/brainshare/showdaily/sun_feature2.html). (Mac 2001).

Chappell, L. (2000). TCP/IP Analysis and Troubleshooting. Protocol Analysis Institute. <http://www.packet-level.com>

Dah Ming Chiu dan Sudama, R. (1992). Network Monitoring Explained. England. Ellis Horwood Limited.

Dickson, G. dan Llyod, A. (1992). Open Systems Interconnection. Australia. Prentice Hall .

Graham, R. (14 september 2000). Sniffing – network wiretap.  
<http://www.robertgraham.com/pubs/sniffing.html>. (7 Februari 2001).

Johnson, A. (2000). Agilent Technologies: Enterprise LAN Monitoring and Analysis. <http://www.agilent.com/comms/onenetworks>. (Feb, 2001)

Iskandar Abdul Rashid dan Zaitun Ismail (2001). Membina Laman WEB menggunakan HTML. Kuala Lumpur, Malaysia. Venton Publishing.



- Leinwand, A. dan Conroy, K. F. (1996). Network Management: A Practical Perspective. USA. Addison-Wesley Pub. Company, Inc.
- Miller, M. A. (1990). LAN Protocol Handbook. USA. M&T Publishing Inc.
- Mohd Majid Konting (1993). Kaedah Penyelidikan Pendidikan. Kuala Lumpur. Dewan Bahasa dan Pustaka.
- Mueller, J. dan William, R. A. (1993). Guide to Network Management. USA. Mc-Graw-Hill
- Murphy, S. (2000). Networking Complete. USA. SYBEX, Network Press.
- Napjus, E. A (2001). Microsoft Networking Problems at Carnegie Mellon.  
<http://www.net.cmu.edu/docss/arch/peerprobs.html>.
- Simon, A. R. dan Wheeler, T. (1995). Open System Handbook (Second Editin). London. Academic Press Inc.
- Steinke, S. (2000). Network Tutorial : A Complete Introduction To Network. USA. CMP Media Inc.
- Storm, D. (Sept, 2000). The Packet Filter: A Basic Network Security Tool. SANS Institute. [http://www.sans.org/infosecFAQ/packet\\_filter.htm](http://www.sans.org/infosecFAQ/packet_filter.htm) (Mac, 2001)
- Tanenbaum, A. S. (1996). Computer Networks (Third Edition). USA. Prentice Hall Inc
- Thomson, A. (2000). Understanding Local Area Networks : A Practical Approach. USA. Prentice-Hall, New Jersey.

Yu Feng (1998). Observing FTP transfer performance by packet analysis.  
Graduation project report. Department of Computer Science Texas A&M  
University, College, Texas.